Commonwealth of Massachusetts
Executive Office of Technology Services and Security (EOTSS)
Enterprise Security Office

Third-party Information Security Standard

Document Name: Third-party Information Security	Effective Date: October 15th, 2018
Document ID: IS.015	Last Revised Date: November 04, 2021

Table of contents

1. PURPOSE

1.1. This ***standard*** establishes security requirements for the use of ***third parties*** that handle Commonwealth ***confidential*** information, either by storing, processing, transmitting or receiving information. This standard outlines the following controls to reduce the information security risks associated with contracted services and staff:

- Identification of risks related to ***third parties*** to ensure appropriate protection of Commonwealth ***information assets***
- Definition of information security requirements for ***third-party*** agreements
- ***Third-party*** information management oversight from contract initiation through termination

2. AUTHORITY

2.1. M.G.L. Ch. 7d provides that "Notwithstanding any general or special law, rule, regulation, executive order, policy or procedure to the contrary, all executive department agencies shall, and other state agencies may, adhere to the policies, procedures and objectives established by the executive office of technology services and security with respect to activities concerning information technology."

3. SCOPE

3.1. This document applies to the use of information, information systems, electronic and computing devices, applications, and network resources used to conduct business on behalf of the Commonwealth. The document applies to the Executive Department including all executive offices, and all boards, commissions, agencies, departments, divisions, councils, and bureaus.. Other Commonwealth entities that voluntarily use or participate in services provided by the Executive Office of Technology Services and Security, such as mass.gov, must agree to comply with this document as a condition of use. Executive Department agencies and offices are required to implement procedures that ensure their ***personnel*** comply with the requirements herein to safeguard information.

4. RESPONSIBILITY

4.1. The Enterprise Security Office is responsible for the development and ongoing maintenance of this ***standard***.

4.2. The Enterprise Security Office is responsible for this ***standard*** and may enlist other departments to assist in the monitoring and maintenance of compliance with this ***standard***.

4.3. Any inquiries or comments regarding this ***standard*** shall be submitted to the Enterprise Security Office by sending an email to **Error! Hyperlink reference not valid.**.

4.4. Additional ***information*** regarding this ***standard*** and its related standards may be found at https://www.mass.gov/cybersecurity/policy.

5. COMPLIANCE

5.1. Compliance with this document is mandatory for the Executive Department including all executive offices, boards, commissions, agencies, departments, divisions, councils, and bureaus. Violations are subject to disciplinary action in accordance to applicable employment and collective bargaining agreements, up to and including the termination of their employment and/or assignment with the Commonwealth.

Exceptions to any part of this document must be requested via email to the Security Office (**Error! Hyperlink reference not valid.**). A policy exception may be granted only if the benefits of the exception outweigh the increased risks, as determined by the Commonwealth CISO.

6. STANDARD STATEMENTS

6.1. Third-party Selection

As part of the ***third-party*** selection process, Commonwealth Offices and Agencies must ensure that the items listed below should be evaluated from a security perspective during the sourcing and contracting phases:

6.1.1. Technical and industry experience

6.1.1.1. Identify areas where the Commonwealth may have to supplement the ***third party***'s capabilities related to information management to fully manage risk to Commonwealth's ***information assets***.

6.1.1.2. Evaluate the ***third party***'s use of other ***third parties***' (i.e., subcontracting relationships) technology to support the contracted operations.

6.1.1.3. Evaluate the experience of the ***third party*** in providing services that include the handling of ***confidential*** information in the anticipated operating environment.

6.1.1.4. Evaluate the ***third party***'s ability to respond to service disruptions (see *Incident Management and Business Continuity and Disaster Recovery* standards).

6.1.2. Operations and control (as applicable)

6.1.2.1. Determine/review the adequacy of the ***third party***'s policies and procedures relating to internal controls in accordance with Report on Controls of Service Organizations such as SOC1/SOC2 User/Client Control Considerations (e.g., parameters, logical access, event logs/audit trails), facilities management, privacy protections, maintenance of records, business resumption contingency planning, secure systems development and maintenance and ***state employee*** background checks.

6.1.2.2. Determine whether the ***third party*** provides sufficient security precautions, including, when appropriate, firewalls, encryption and customer identity authentication, to protect Commonwealth information resources as well as detect and respond to intrusions.

6.1.2.3. Evaluate whether the Commonwealth has complete and timely access to its information maintained by the ***third party*** both during and after any third party engagement.

6.1.2.4. Evaluate the ***third party***'s knowledge of regulations (e.g., PHI, PCI) that are relevant to the services they are providing.

6.1.2.5. Assess the adequacy of the ***third party***'s insurance coverage in consultation with risk management or procurement functions.

6.2. Contractual Security Risk Identification

All contracts by which a ***third party*** provides services to the Commonwealth or allows a ***third party*** to access, store, process, analyze or transmit Commonwealth ***confidential information*** shall be assessed, prior to entering into an agreement, to determine the ***third party***'s capability to maintain the confidentiality, integrity and availability of Commonwealth ***information assets*** consistent with the Enterprise *Information Protection Requirements Standard*. The following shall be considered during ***third-party*** sourcing and/or contract negotiation:

6.2.1. ***Third-party*** sourcing and contract negotiation

6.2.1.1. Organizational objectives and requirements.

6.2.1.2. Transparency to evaluate and manage ***third-party*** relationships.

6.2.1.3. Importance and criticality of the services to the Commonwealth (see *Asset Management and Communication and Network Security Standard)*.

6.2.1.4. Defined requirements for the contracting activity, including any potential regulatory requirements.

6.2.1.5. Necessary security controls/reporting processes in Commonwealth Executive Offices and Agencies.

6.2.1.6. Contractual obligations and requirements to be imposed on the ***third party***.

6.2.1.7. Contingency plans, including the availability of alternate ***third parties***, costs and resources required to switch ***third parties*** upon breach or termination (see *IS.005 Business Continuity and Disaster Recovery* standards)

6.3. Contractual Security Provisions

Commonwealth Offices and Agencies must ensure that Information Security policies and requirements are addressed and documented in any contract with the ***third party***. Provisions shall be established in the contract to protect the security of the Commonwealth's ***information assets***.

6.3.1. ***Third-party*** contracts must address the following, where applicable:

6.3.1.1. All parties involved with the agreement must be made aware of their privacy and security responsibilities and are required to sign confidentiality agreements (e.g., non-disclosure agreement).

6.3.1.2. Information classification requirements in accordance with the Commonwealth's *Information Classification* and *Information Protection Requirements* standards.

6.3.1.3. Relevant legal and regulatory requirements which may apply to information processed, stored or transmitted.

6.3.1.4. Requirements governing the acceptable use of Commonwealth-owned or managed information.

6.3.1.5. The means by which a ***third party*** proposes to transfer information to other ***third parties*** and will require written notice and agreement from Commonwealth prior to any such transfer.

6.3.1.6. Adherence by the ***third party*** to an information security program, including, but not limited to, password and access management requirements, physical security of facilities and servers containing Commonwealth information, network protection, system and software protection, encryption and information security of data in transit and at rest, and intrusion-detection/prevention systems.

6.3.1.7. Training and awareness requirements for specific procedures and information security requirements (e.g., for incident response, authorization procedures).

6.3.1.8. Screening requirements, if any, for ***third-party*** personnel, including responsibilities for conducting the screening and notification procedures if screening has not been completed or if the results give cause for concern.

6.3.1.9. Commonwealth's explicit reserved right to audit the performance of information security and other contractual responsibilities of the parties involved in the signed agreement. This will be done when deemed necessary by a Commonwealth organization, and doing so will incur no additional cost to a Commonwealth's contract.

6.3.1.10. ***Third party***'s obligation to periodically deliver an independent report on the effectiveness of controls (e.g., SOC1/SOC2, vulnerability testing results) and agreement on timely correction of relevant issues raised in the report.

6.3.1.11. Processes used by the ***third party*** to report incidents in writing to the Commonwealth involving any type of security breach or unauthorized access to the Commonwealth's ***information assets*** within the appropriate timeframes (see *Incident Management Standard*).

6.3.1.12. Upon termination of the contract, Commonwealth information will be transmitted to the Commonwealth or the Commonwealth's ***third party*** of choice in a format defined by the Commonwealth at a cost specified to the mutual satisfaction of the Commonwealth and the third party prior to termination.

6.3.1.13. Processes used to electronically erase, render unreadable or physically destroy all Commonwealth's information assets upon termination of the agreement (see *Information Disposal Standard*).

6.3.1.14. Commonwealth's explicit reserved right to request, at any time, transfer or purging of some or all information stored on ***third-party*** systems at a cost specified to the mutual satisfaction of the Commonwealth and the third party prior to termination.

6.3.1.15. Maintenance and testing procedures for Business Continuity Planning as appropriate.

6.3.1.16. Enabling processes to provide for timely forensic investigation in the event of a compromise.

All contracts shall be reviewed according to each agency's internal policy. If the information being collected or exchanged is ***confidential***, a binding non-disclosure agreement shall be in place between the Commonwealth and the ***third party***, whether as part of the contract or a separate non-disclosure agreement (required before any confidential information is shared).

6.4. Third party Life Cycle Management

Commonwealth Offices and Agencies must ensure that all ***third parties*** shall be managed through the life cycle of the contract by the ***Information Owner*** in collaboration with the Information Security Team and Procurement/Legal.

6.4.1. The following shall be considered throughout the ***third-party*** life cycle management process:

6.4.1.1. Inventory of ***third parties*** with assigned vendor risk rating.

6.4.1.2. Contractual performance criteria or service-level agreements.

6.4.1.3. Contractual, regulatory or legal requirements.

6.4.1.4. Inventory of all relevant contractual deliverables.

6.4.1.5. Information classification of information entrusted to ***third parties***.

6.4.1.6. Enablement of accounts used by ***third parties*** for remote access only during the time period needed and monitor remote access accounts when in use.

6.4.1.7. Audit provisions to determine the ***third party***'s compliance per defined requirements.

6.4.1.8. The frequency of audit based on advice from functions such as Internal Audit, Information Security and Legal.

6.4.1.9. Communicate the need for transition or return of information at end of engagement/contract and obtain certification in writing from the ***third party*** that all Commonwealth information has been permanently deleted if the contract so requires.

6.4.1.10. Risk assessment at the onset and at least annually thereafter and upon significant changes to the agreement or environment. The risk assessment shall identify critical assets, threats and vulnerabilities and result in a formal, documented analysis of risk (*see Risk Management Standard).* Significant changes include:

6.4.1.10.1. Changes and enhancement to networks.

6.4.1.10.2. Use of new technologies.

6.4.1.10.3. Adoption of new products or newer versions or releases.

6.4.1.10.4. New development tools and environments.

6.4.1.10.5. Changes to the physical location of service facilities.

6.4.1.10.6. Subcontracting to another ***third party.***

6.4.1.11. Awareness training for Commonwealth personnel that interact with ***third parties*** regarding appropriate rules of engagement based on the type of ***third party*** and level of access to Commonwealth ***information assets***.

7. CONTROL MAPPING

Section	NIST SP800-53 R5	CIS 18 v8	NIST CSF
6.1 Third-party Selection	SR-1	CSC 15	
6.2 Contractual Security Risk Identification	SR-2	-	
6.3 Contractual Security Provisions	SR-5	CSC 15	
	SR-8	-	
	SR-3	-	
6.4. Third-party Life Cycle	SR-10	-	
	SR-11	CSC 16	

8. RELATED DOCUMENTS

Document	Effective date

9. DOCUMENT CHANGE CONTROL

Version No.	Revised by	Effective date	Description of changes
0.9	Jim Cusson	10/01/2017	Corrections and formatting.
0.92	John Merto	01/02/2018	Corrections
0.95	Sean Vinck	5/7/2018	Corrections and formatting.
0.97	Andrew Rudder	5/31/2018	Corrections and formatting
0.98	Anthony O'Neill	05/31/2018	Corrections and Formatting
1.0	Dennis McDermitt	06/01/2018	Pre-publication review
1.0	Andrew Rudder	10/4/2018	Approved for Publication by: John Merto
1.1	Megan Perkins	7/15/2020	Annual Review; Minor corrections and formatting
1.2	Sean M. Hughes	11/04/2021	Annual Review
1.3	Sean M. Hughes	08/29/2022	Updates for 800-53r5 and Annual Review

The owner of this document is the Commonwealth CISO (or designee). It is the responsibility of the document owner to maintain, update and communicate the content of this document. Questions or suggestions for improvement shall be submitted to the document owner.

9.1 Annual Review

This ***Third-party*** *Information Security Standard* shall be reviewed and updated by the document owner on an annual basis or when significant *Standard* or procedure changes necessitate an amendment.